OZY

FAST FORWARD

THE FUTURE OF CRIME IN THE BLOCKCHAIN ECONOMY

WHY YOU SHOULD CARE

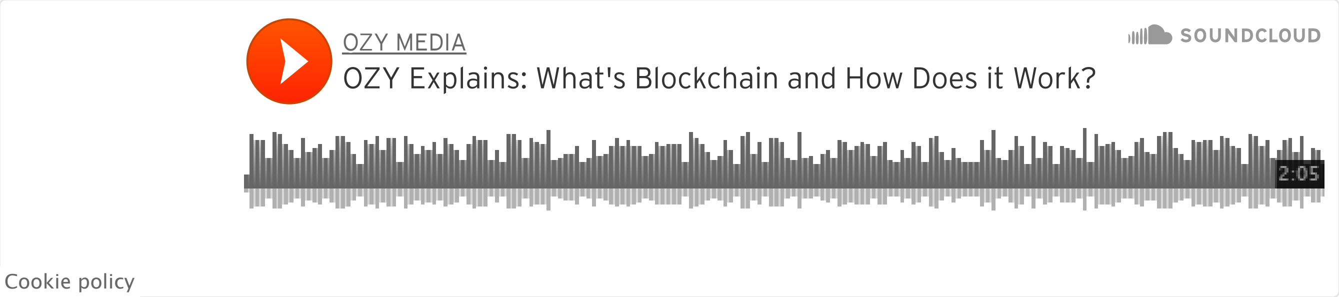
Because everything from your bank to your government will soon be using this tech — and so will criminals.

By James Watkins

THE DAILY DOSE OCT 17 2017

It all started with an online marketplace to buy drugs. Well, it had started a couple of years before that, but the darknet outfit known as Silk Road was the first time most people heard about bitcoin and cryptocurrency. After doing more than a billion dollars' worth of trades in a little more than two years, Silk Road was shut down in 2013 following an FBI investigation. Despite this shady origin story, the technology behind the drug bazaar's currency — blockchain — is now being touted as the most disruptive technology since the internet.

Blockchain is a way of digitally recording transactions in a universally shared and unchangeable ledger. And, like the internet, it is becoming a major part of the world's digital infrastructure, from finance to health to public services, without shedding tagalong crime. If anything, "we're just seeing the tip of the iceberg when it comes to crime," says Jackson Palmer, a San Francisco–based project manager who shot to prominence in the crypto world as the creator of dogecoin, a cryptocurrency that now has a nine-figure market cap. "Dark-market usage represents quite a small percentage" of cryptocurrency exchanges, now that speculative trading and crowdfunding-style initial coin offerings (ICOs) for startups have taken off, says Palmer, but in crimes like money laundering, phishing and good old-fashioned hacking, the fun might only just be starting.


OZY MEDIA

OZY Explains: What's Blockchain and How Does it Work?

At the heart of blockchain — and the cryptocurrencies built atop it — is an unchangeable chronological list of all transactions in the system. And so, in theory, law enforcement has more to go on when investigating money laundering or the purchase of illicit goods with cryptocurrencies than with, say, cash. "Criminals don't need to use cryptocurrencies because they have cash and … the banking system," says Alan Cohn, counsel to the Blockchain Alliance, a public-private forum of blockchain businesses and law enforcement. The criminals behind Silk Road were eventually brought down by tracking payments on the public Bitcoin blockchain ledger — the analysis even rumbled two undercover federal agents who had gone rogue. So while "it's certainly possible to launder money using cryptocurrency," says Cohn, the handlers of cryptocurrencies face the same regulatory requirements as a traditional money services business.

IN ALL, ROUGHLY 10 PERCENT OF MONEY INVESTED IN ETHEREUM-BASED ICOS SO FAR IN 2017 HAS ENDED UP IN THE HANDS OF CRIMINALS.

Special software is required to sift through information on public blockchain ledgers and interpret which transactions appear suspicious, and that's getting more difficult as "the bad guys are moving into the more and more anonymous [currencies]," says Camilla Frost, a product manager at Chainalysis, which provided such software for the Silk Road investigation. A recent report from Europol, the EU's policing agency, stated that "cryptocurrencies such as Monero, Ethereum and Zcash are … gaining popularity within the digital underground." Offering advanced privacy features, both Monero and Zcash hide the sender, receiver and value of all transactions, making it nearly impossible to track within the system. (The team behind Zcash insists that just because there is increased privacy doesn't mean there's any evidence of criminal usage; indeed, the Europol report acknowledges that "Zcash has yet to feature in any reported law enforcement investigations.")

Despite the additional privacy available, "the trigger is once [criminals] try to cash out" into usable dollars or euros, says Frost — transactions which, in regulated exchanges, are traceable. *Unregulated* exchanges, though, are a different matter: In July, the Department of Justice indicted a man for laundering more than $4 billion in criminal cash via his black-market cryptoexchange, BTC-e, which did not comply with U.S. regulations.

Russian Alexander Vinnik (center) headed BTC-e, an exchange he operated for the bitcoin cryptocurrency. He was indicted by a U.S. court in July on 21 charges ranging from identity theft and facilitating drug trafficking to money laundering.

SOURCE NICOLAS ECONOMOU/GETTY

As for criminal activity on or against the networks themselves, “phishing is a major trend,” says Frost, whose Chainalysis research found evidence of more than $115 million worth of stolen value affecting nearly 17,000 victims on the Ethereum blockchain alone. Just like following a dodgy email link that pretends to be your bank, cryptophishing usually involves suckering investors into sending money to the wrong address for a supposed presale of coins in an ICO, with Twitter often used to spread the misinformation. Allegations of selling based on misinformation and Ponzi schemes are also rife in the ICO space.

To date, there have been no cases of a major blockchain itself getting hacked, but the code behind the applications built on top of that infrastructure is also a vulnerability. In 2016, a crowdfunded venture capital fund called the DAO raised more than $150 million in a month (at the time, the largest crowdfunding event in history) — and a month later thieves exploited a vulnerability in the DAO code to steal more than $74 million from 11,000 investors. In all, roughly 10 percent of money invested in Ethereum-based ICOs so far in 2017 has ended up in the hands of criminals, estimates Chainalysis.

Despite the security credentials of blockchain, the technology is not necessarily *perfectly* secure — and if it’s not, the consequences could be devastating. Given the value now stacked on a few major blockchains (primarily, Bitcoin and Ethereum), “you’re placing the world’s biggest bug bounty on that network,” says Palmer. “The code itself has to be absolutely rock-solid” — and open-source software only makes the search for vulnerabilities easier. If a software bug on the scale of the 2014 “Heartbleed” bug is found in Ethereum, says Palmer, “we could be talking about billions of dollars being stolen, siphoned off by hackers before people know about it.”

And while phishing and hacking threats are present in any technology-supported marketplace, there is a big gray area in the ICO space because regulators have yet to decide exactly what a cryptotoken *is*. It can have characteristics of “a currency and a commodity and a security and property," says Cohn, because of the equity or other rights that come with the purchase of some coins. This regulatory uncertainty means coin creators are engaging in all manner of shady practices, including the alleged secret sale of leftover tokens to existing investors at a lower price — a practice that would be a felony on Wall Street, according to *Forbes*.

"It's always going to be a cat-and-mouse game between law enforcement and criminals," says Cohn. And in the new Wild West of the digital economy, it's game on.

SEE BEYOND